CHAPTER-7
Application Scope and Future Trend

7.1 Chapter Overview
In this chapter researcher focus research advantage and disadvantage, future research in this area.

7.2 Application advantages and disadvantage
- Apply to network-based navigation and predication
- Apply to handset-based navigation and predication
- Apply to SIM-based navigation and prediction
- Predict to CDRs base navigation
- Help to build a advanced technology for GSM/CDMA navigation and CDRs analysis
- Complication of CDRs analysis is need to technical skill

7.3 Scope
The primary scopes of the present research are as follows:
- Criminal suspect monitoring and nature prediction
- Advance Police Control System
- Prevention of misuse of cell phone
- Miscellaneous Applications after implementation.

7.4 Future trend and Scope
Cellphone digital data and network data (like CDR) such, investigation is a reactive field, and as such future trends in cell phone network CDR analysis are largely dependent on trends in the cellphone industry. Cellphones are becoming much more capable and CDR data it can more incremental growth with WAP application cellphones with greater functionality are the expanding market. The term smart phone is ceasing to be relevant as it becomes the standard. For network investigation and analysts, this is positive for two reasons, cellphone will have greater capability and hence will contain more potential evidence, and the industry is stabilizing to a smaller number of core operating system platforms.
The propagation of high-tech smart cellphone in both the consumer and commercial sectors will ultimately have an impact on investigation. The increased capacity of phones will require greater analysis on a per-device basis but can provide greater insight. Cell phones are a data store largely abstracted away from individual users and are less likely to be altered or tampered with. The number of mobile phone and device operating systems is consolidating to a discrete group, largely independent of the hardware. This will aid data extraction and analysis in reduced learning curves for different devices as well as a greater understanding of what can be extracted for each platform.

The need to reverse-engineer or re-engineering of technology the idiosyncrasies found in custom operating systems or individual implementations will decrease over time. The future of cell phone and device investigation analysis will, to a greater degree, involve the reengineering of third party applications. Such applications are platform-dependent, written either with native SDKs or through third-party tool sets, and have differing access to the underlying operating system. Understanding the capability and intent of third-party applications may be vital to investigation analysts in certain circumstances, as they may be malicious in nature, indirectly facilitate crime, provide communication mechanisms outside of standard on-phone systems, or store data of investigation value (either locally or on externally hosted servers). Third-party applications are also likely gateways to cloud services, which are increasingly catering to mobile devices.

The investigation implications of cloud computing are beyond the scope of this work, but you must be aware of both their existence and the idea that evidence exists beyond the device itself. Low-end phones with basic functionality will continue to exist in significant numbers. From a digital investigation perspective, these phones are cheap and disposable, and it is difficult to attribute ownership. Such analysis needs greater scalability in analysis, for situations where an individual may control multiple phones, multiple groups control a single phone, and for large-scale social network analysis. Current links between workstations and notebook computers and phones almost exclusively view the phone as a satellite device.
Improved connectivity between phones and other data sources may alter this and provide
greater links between connected systems. By far the most obvious trend is that mobile devices
will continue to be important in investigation analysis and have a large role in both civil and
criminal investigations. With increased connectivity options and higher storage capacities and
processing power, abuse of cell phones can become more mainstream. Mobile phones outsell
personal computers and with digital crime rates rising, the mobile phone may be the next avenue
for abuse for digital crime. Mobile phones with their increased connectivity options may become
a source of viruses that infect computers and spread on the internet.

Virus writers typically look for operating systems that are widely used. This is because
they want their attacks to have the most impact. When it comes to mobile phones and their
operating systems, there appears to be certain operating systems that are dominating the market
which makes them a prime candidate for attacks. According to recent studies, phone virus and
malware infection rates are expected to increase with newer smart phones. Mobile phone
technology is evolving at a rapid pace. Digital investigation relating to mobile devices seems to
be at a standstill or evolving slowly. For mobile phone investigation to catch up with release
cycles of mobile phones, more comprehensive and in-depth framework for evaluating mobile
investigation toolkits should be developed and data on appropriate tools and techniques for each
type of phone should be made available in a timely manner. Future trends in mobile phone devices
and their components can be divided into processor speed and components, battery types and
technologies affecting them, and finally, memory and storage capacities. All of these
components and their developments may have an impact on mobile device investigation.
Processor Components and Speed Intel has already demonstrated a 1GHz processor for mobile
devices. In addition to this high processing speed, smart mobile phone devices are showing the
trend of using System on Chip (SoC) technology. This technology allows the processor to
incorporate a set of distinct functionalities in the same package which reduces the number of
chips required by it as well as incorporating a considerable amount of built-in memory. This
change in processor architecture may have an undesirable impact on mobile investigation.

Cell phone device investigation is an ever-evolving field filled with challenges and
opportunities when analyzing a mobile device for investigation evidence in support of a criminal
investigation. The process can be more difficult than traditional computer investigation due to
the volatile nature of electronic evidence. A well trained, highly skilled digital investigation investigator plays an essential role in the criminal investigation process when performing investigation analysis of mobile devices that belong to suspects, witnesses, victims or through the analysis of network. Although investigation toolkits do exist for the investigator, the majority of the tools are either not fully developed and do not yet provide full functionality for multiple devices. Budget constraints of law enforcement departments prohibit the purchase of quality software packages to use with the varying mobile device manufacturers.

The key is for the investigator to use the appropriate toolset that is meant for that particular purpose in performing investigation analysis in an effective manner that will support a criminal case. Even such a pertinent piece of investigation equipment, like the Faraday bag for the first-responder, is not free from issue. Once removed from the Faraday bag, a mobile device can start receiving data if powered on and be able to connect to the network. This may be difficult to control for the first responder if he is instructed by a higher official to leave the mobile device powered on upon discovery at the crime scene. Some devices can be controlled by placing the phone in airplane mode, thus disabling the wireless features, but not all mobile devices possess this functionality. For the most part, Faraday bags are reliable but cannot fully guarantee that a signal will not reach the phone. Successfully blocking the signal depends upon the quality of the bag, the distance to the cell tower, and the power of the transmitter in the mobile device. Another challenge that faces the investigation investigator is digital evidence that is obtained for a criminal investigation can be preceded by a suppression hearing. A suppression hearing is an opportunity for a judge to look at the evidence and determine whether it will be admissible or violates the suppression of evidence which determines if an unreasonable search or seizure violated a defendant’s constitutional right.

Investigation computing continues to play an increasingly important role in civil litigations, especially in electronic discovery, intellectual property (IP) disputes, as well as information security and employment law disputes. Investigation investigators must be aware of certain issues pertaining to data acquisition and the preservation of digital evidence for a criminal investigation. Electronic data is very susceptible to alteration or deletion, whether through an intentional change or from the result of an invoked application in some computing process. As
electronic data is created, modified or deleted through the normal operations of a computing system, there lies the possibility of modifications arising from an incorrect or inappropriate digital investigation process. Given that the results of such actions can be treated as critical evidence in a case, it is essential that every measure be taken to ensure the reliability and accuracy of the investigation process. A digital investigation process must be developed and applied with due regard to jurisprudence issues. It is imperative that the digital investigation process is capable of being examined thoroughly to determine the reasonableness and reliability to refrain from being admissible.